Risk Management and Cyber Threat Mitigation

Leading and Managing Enterprise Information Security

March 2025

Holli Meyers
University of Washington

Introduction

Let’s review a recent cyber threat that has impacted critical infrastructure.

Schneider Electric

A French multinational company in the electricity sector. Employs over 100,000 individuals and generates around $40 billion annually.

Services and Products

Offers training courses, consulting, equipment support, management software, electrical and automation products, and control and monitoring systems.

Stakeholders

Serves industries in agriculture, healthcare, engineering, aerospace, automotive, electronics, apparel, maritime, and more.

(Abrams; “Company Profile”; “Industries Served - Schneider Electric”)

Hellcat Ransomware Group

November 4th, 2024

Schneider’s custom project management server (Atlassian Jira) and developer platform (Gravatar), hosted in an isolated environment, were infiltrated using exposed credentials.

The Jira server is configured with a REST API authentication add-on, miniOrange. Through the plugin Hellcat scraped 400,000 rows of data and demanded $125,000 in exchange.

Compromised data included names, email addresses, project files, and plugin information.

The data was released for direct download on Hellcat’s Onion domain sometime between November and December.

(Abrams; Greig; Jones; “REST API Authentication”; TheRavenFile; Swain)

Regulatory Standards

Here are a few of Schneider Electric’s 40 cybersecurity policies and standards.

ISO 27001

Information security management.

ISO 30111:2019 / 29147:2018

Vulnerability handling and disclosure.

NIST CSF

Risk management framework.

GDPR

General data protection regulation.

ISA/IEC 62443

Industrial control systems security.

(“Securing Critical Infrastructure” 6; “2022 Universal Registration Document” 123)

Regulatory Standards

Security notices following the attack:

CWE	
862	Missing Authentication
119	Improper Restriction of Operations with Bound Memory Buffer
924	Improper Enforcement of Message Integrity During Transmission in a Communication Channel
640	Weak Forgotten Password Recovery Mechanism
400	Uncontrolled Resource Consumption
290	Authentication Bypass by Spoofing
20	Improper Input Validation
287	Improper Authorization

ISO 27001

Information security management.

ISO 30111:2019 / 29147:2018

Vulnerability handling and disclosure.

NIST CSF

Risk management framework.

GDPR

General data protection regulation.

ISA/IEC 62443

Industrial control systems security.

(Modicon Reports SEVD-2024-317-02, -03; PowerLogic PM5300, PM5500; EcoStruxure 1)

Regulatory Standards

Security notices following the attack:

CWE	
862	Missing Authentication
119	Improper Restriction of Operations with Bound Memory Buffer
924	Improper Enforcement of Message Integrity During Transmission in a Communication Channel
640	Weak Forgotten Password Recovery Mechanism
400	Uncontrolled Resource Consumption
290	Authentication Bypass by Spoofing
20	Improper Input Validation
287	Improper Authorization

ISO 27001

Access control, password management, and security.

ISO 30111:2019 / 29147:2018

Vulnerability handling and disclosure.

NIST CSF

Data integrity and identity/authentication proofing.

GDPR

Data protection, availability, and security of processing.

ISA/IEC 62443

Authorization, session integrity, and authentication.

(Modicon Reports SEVD-2024-317-02, -03; PowerLogic PM5300, PM5500; EcoStruxure 1)

Industry Perspective

VP of Electrical Operations

How does the company spread employee awareness on cybersecurity risks?
“We have quarterly trainings with our employees. We also will send fake emails to our employees to see if they open or notify IT.”

Have you experienced any cyber threats in your job?
“Yes, our accounting department opened an email with an attachment, that attachment ended up being malicious. We ended up having to pay ransom.”

How would the company handle a data breach?
“Our cyber practices involve investigating what we can and submitting a report to our insurance carrier. As a preventative measure, we try to not keep too much highly sensitive data in our systems and consistently backup what remaining information we have.”

Response and Mitigation Recommendations

1

Strengthen **XDR solutions** to provide better end-to-end network visibility and eliminate blind spots.

2

Improve **training and education** programs to prevent exposures related to human error.

3

Expand **NDR solutions** to enhance network traffic and suspicious activity monitoring.

4

Promoting **active management practices** by setting up creative, adaptable cybersecurity experts for success is vital for securing the company’s assets.

(Sangfor Technologies; Swain)

Works Cited

01 Abrams, Lawrence. “Schneider Electric confirms dev platform breach after hacker steals data.” *BleepingComputer*, 4 Nov. 2024, www.bleepingcomputer.com/news/security/schneider-electric-confirms-dev-platform-breach-after-hacker-steals-data/. Accessed 20 Jan. 2025.

02 “Company Profile.” *Schneider Electric*, www.se.com/us/en/about-us/company-profile/.

03 *EcoStruxure IT Gateway.* Schneider Electric Security Notification, 12 Nov. 2024. Report no. SEVD-2024-317-04. https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-

04 31704&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-317-04.pdf, PDF file.

05 “Industries Served - Schneider Electric.” *Schneider Electric*, 24 July 2019, www.schneiderelectricrepair.com/industries-served/. Accessed 7 Mar. 2025.

06 *Modicon Controllers M340 / Momentum / MC80.* Schneider Electric Security Notification, 12 Nov. 2024. Report no. SEVD-2024-317-03. https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-317-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-317-03.pdf, PDF file.

07 ---. Report no. SEVD-2024-317-02. https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-317-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-317-02.pdf, PDF file.

Works Cited

08 *PowerLogic PM5500 and PowerLogic PM8ECC*. Schneider Electric, Security Notification, 12 Nov. 2024. Report no. SEVVD-2021-159-02. https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-159-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2021-159- 02.pdf, PDF file.

09 "REST API Authentication." *Atlassian*, 18 Oct. 2023, www.miniorange.com/atlassian/rest-api-authentication. Accessed 7 Mar. 2025.

10 Sangfor Technologies. "Schneider Electric data breach by Hellcat Ransomware Gang." *Sangfor,* 8 Nov. 2024, www.sangfor.com/blog/cybersecurity/schneider-electric-data-breach-hellcat-ransomware-gang. Accessed 20 Jan. 2025.

11 *Securing Critical Infrastructure Through Zones of Influence: People, Company, Supplier/Partners, and Customers.* Schneider Electric, Cybersecurity Posture Paper. https://download.schneider-electric.com/files?p_Doc_Ref=SECyberSecurity&p_enDocType=Institutional+Document#page=3, PDF file.

12 Swain, Gyana. "Schneider Electric suffers data breach, exposing critical project and user data." *CSO,* 6 Nov. 2024, https://www.csoonline.com/article/3599966/schneider-electric-suffers-data-breach-exposing-critical-project-and-user-data.html. Accessed 20 Jan. 2025.

Works Cited

13 TheRavenFile. “IOC / Hellcat Ransomware.” *GitHub,* https://github.com/TheRavenFile/IOC/blob/main/Hellcat%20Ransomware. Accessed 21 Jan. 2025.

14 *2022 Universal Registration Document.* Schneider Electric, Financial and Sustainable Development Report, 2022. https://flipbook.se.com/ww/en/998-22385455/2023/#page/125, PDF file.